SAFE WEB SURFING

The Internet used to be a safe place, but over time, web pages became more and more interactive. Today, the Internet is full of hazards and it is up to you to protect yourself from the criminals who intend to harm you. The danger lies in the potential impact web browsing can have on your personal identity and financial standing.

Every computer connected to the Net is a target of intrusive adware, malware, viruses and phishing (masquerading as a legitimate business), all of which are secretly and routinely installed onto personal computers without the user's knowledge. The nefarious individuals behind these intrusive and invasive software programs have one purpose in mind: to collect personal information about you and make money from what they learn about you.

Anyone who uses the Internet should evaluate how they use the Web and educate themselves about how to avoid disclosing personal information when they use the Internet at home, at work, or on the go. The following tips will help you have a safer Web browsing experience.

1. **Keep everything updated** - This includes your web browser, antivirus software, operating system and the individual software programs you purchased. Conduct regular anti-virus and malware scans of your computer.

2. **Use a firewall** – Firewalls monitor traffic between your computer or network and the Internet and are your first and best line of defense. Most operating systems and routers come with a firewall, but it won't help you if you don't activate it or you disable it.

3. **Secure wireless networks** – The first line of defense for your Wi-Fi network is encryption, which encodes the data transmitted between your PC and your wireless router. Make sure you change the default network name and password on your router. Doing so will make it much more difficult for hackers to break into your router and commandeer its settings. And don't forget to enable the firewall on your router and regularly change the router's administrative password. Check the support section of your ISP's website or your router manufacturer's website for instructions on how to take these precautionary steps. When surfing with a mobile device, ensure you always use a secure wireless connection (one that requires a password). Beware of free wireless hotspots.

4. **Click with caution** – Be careful when you click on links in email messages, on social networking sites and even in search results as they could connect you to phony websites designed to solicit personal information, or they could embed malware on your computer or mobile device designed to steal personal information.

5. **Practice safe shopping** – Shopping online can be a great experience, but be careful. Evaluate the site's security and privacy policies regarding the use of your personal data. Always look for the "https" prefix in the URL or the lock symbol that verifies that the page is encrypted or scrambled. Use a credit card instead of a debit card; if the site turns out to be fraudulent, your credit card company may reimburse you for the charges.

6. **Beware of infected websites -** Attackers are increasingly infecting legitimate websites with malicious code by exploiting a vulnerability in the web server or other software. Your computer can be compromised by visiting a legitimate or "trusted" website that has been infected. So even sticking to trusted websites won't guarantee your computer's safety.

7. **Download with caution -** Be careful about downloading any software file off the Internet! Adware, malware and viruses frequently embedded in music, video and other files. As a rule of thumb, only download files from trusted sources and check them with your anti-virus software, since even a trusted source might be infected. To do this, select the Save option instead of the Open option and scan the file with your anti-virus program before opening or installing it.

8. **Disable pop-up windows -** Attackers can use popup windows that look like offers, but their purpose is to install malicious code. Pop-up window are also frequently used to display annoying or even offensive content. Disabling popup windows can be a reasonable step to more comfortable web browsing.

9. **Control who uses your computer -** Children and teenagers are frequently unaware that their music, games and video downloads can be dangerous. In general, assume that anyone other than you using your computer does not know how to surf safely. Their lack of knowledge could be dangerous.

10. **Be skeptical** – Many victims of scams may have thought they were cyber savvy and let their guard drop long enough for a cybercriminal to strike. Back up data regularly in case a virus infects your computer, and monitor accounts and credit reports to make sure your identity has not been stolen.

Cybercrime continues to accelerate and it's being fueled by common mistakes people make when online. Use common sense and caution and your Web surfing experience should remain a pleasant one.

Your financial institution has taken strong measures to ensure the security and safety of your account and its overall online banking system. By staying alert to potential security threats and keeping in mind the suggestions listed above, you can help us keep online banking extremely safe and secure. Follow the good practices and use the knowledge we've provided here, and you will be much more prepared to enjoy the conveniences of online services with peace of mind!

These helpful tips are provided by www.infosightinc.com, a computer security company working with your bank to help insure the privacy and security of your financial information.